CLAIMS

1. A key distribution system for distributing shared keys, said key distribution system comprising:

a server which generates common information based on each of the shared keys and distributes the common information; and

receiving devices each of which obtains the shared key based on the common information and an individual intermediate key group set,

wherein each of said receiving devices has been previously provided with at least one individual intermediate key group set which has been selected from among individual intermediate key group sets including at least two different types of individual intermediate key group sets, each of the individual intermediate key group sets including individual intermediate key groups, and each of the individual intermediate key groups being made up of one or more individual intermediate keys which have been generated based on one or more system secret variable groups,

said server and said receiving devices can communicate via a communication channel,

said server includes:

a shared key storage unit operable to store the shared keys;

a system secret variable group storage unit operable to store the system secret variable group sets which are made up of the previously provided system secret variable groups;

each of common information generation units operable to generate the common information based on each shared key;

a common information generation unit selection unit operable to select one of said common information generation units; and

a common information distribution unit operable to distribute the common information to said receiving devices simultaneously or at different times,

each of said common information generation units is operable to generate key update data based on the system secret variable group set and the shared key and operable to generate, using a different common information generation method, common information including (a) a common information identifier and (b) the key update data, the common information identifier corresponding to the common information generation method,

each of said receiving devices includes:

a common information receiving unit operable to receive the common information;

an individual intermediate key group storage unit operable to store the individual intermediate key group sets each of which is made up of the individual intermediate key groups corresponding to each of the common information generation methods;

shared key obtainment units which respectively correspond to said common information generation units; and

a shared key obtainment unit selection unit operable to select one of said shared key obtainment units,

said shared key obtainment unit selection unit is operable to select one of said shared key obtainment units based on the common information identifier included in the common information which has been received by said common information receiving unit, and

each of said shared key obtainment units is operable to obtain the shared key, using the common information, based on the shared key obtainment method corresponding to the common information identifier and the individual intermediate key group.

2. The key distribution system according to Claim 1,

wherein each common information generation method includes a first common information generation method,

each shared key obtainment method includes a first shared key obtainment method which is paired with the first common information generation method,

each of the system secret variable group sets includes first system secret variable groups each of which is made up of one or more first system secret variables,

each of the individual intermediate key group sets includes first individual intermediate key groups each of which is made up of one or more first individual intermediate keys, the first individual intermediate keys are respectively generated based on the first system secret variable groups and one or more first individual intermediate key generation equations,

said server has been previously provided with one or more time variable generation equations and one or more server shared intermediate key generation equations,

each of said receiving devices has been previously provided with one or more receiving device shared intermediate key generation equations,

the first common information generation method includes:

generating a random number group which is made up of one or more random numbers;

generating a time variable group which is made up of one or more time variables based on the random number group, the first system secret variable groups and the time variable generation equations;

generating shared intermediate keys based on the first system secret variable groups, the random number group and the server shared intermediate key generation equations; and

generating encrypted shared keys by encrypting the shared keys based on the shared intermediate keys,

wherein, in the first common information generation method, the key update data includes the time variable group and the encrypted shared keys, and

the first shared key obtainment method includes:

generating the shared intermediate keys based on the time variable group, the first individual intermediate key group and the receiving device shared intermediate key generation equations; and

obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

3. The key distribution system according to Claim 1,

wherein said server has been previously provided with one of the individual intermediate key group sets,

said server includes an individual intermediate key group set storage unit operable to store the previously provided individual intermediate key group set,

each common information generation method includes a first common information generation method,

each shared key obtainment method includes a first shared key obtainment method which is paired with the first common information generation method,

each of the system secret variable group sets includes first system secret variable groups each of which is made up of one or more first system secret variables,

each of the individual intermediate key group sets includes first individual intermediate key groups each of which is made up of one or more first individual intermediate keys, the first individual intermediate keys are respectively generated based on the first system secret variable groups and one or more first individual intermediate key generation equations,

said server has been previously provided with one or more time variable generation equations and one or more receiving device shared intermediate key generation equations,

each of said receiving devices has been previously provided with the receiving device shared intermediate key generation equations, the first common information generation method includes:

generating a random number group which is made up of one or more random numbers;

generating a time variable group which is made up of one or more time variables based on the random number group, the first system secret variable groups and the time variable generation equations;

generating shared intermediate keys based on the first individual intermediate key group, the time variable group and the receiving device shared intermediate key generation equations; and

generating encrypted shared keys by encrypting the shared keys based on the shared intermediate keys,

wherein, in the first common information generation method, the key update data includes the time variable group and the encrypted shared keys, and

the first shared key obtainment method includes:

generating the shared intermediate keys based on the time variable group, the first individual intermediate key groups and the receiving device shared intermediate key generation equations; and

obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

4. The key distribution system according to Claim 1,

wherein each common information generation method includes a second common information generation method,

each shared key obtainment method includes a second shared key obtainment method which is paired with the second common information generation method,

each of the system secret variable group sets includes a second system secret key group which is made up of second system secret keys,

each of the individual intermediate key group sets includes second individual intermediate key groups each of which is made up of one or more of the second system secret keys,

the second common information generation method includes:

generating encrypted shared keys by encrypting the shared keys based on one or more of the second system secret keys which are included in the second system secret key groups; and

generating an encrypted shared key group which is made up of the encrypted shared keys combined with each other,

wherein, in the second common information generation method, the key update data includes the encrypted shared key group, and

the second shared key obtainment method includes:

selecting one of the encrypted shared keys which corresponds to any of the second system secret keys included in the second individual intermediate key group, from among the encrypted shared key group included in the key update data; and

obtaining the shared key by decrypting the selected encrypted shared key based on the second system secret key.

5. The key distribution system according to Claim 4,

wherein the individual intermediate key group set includes a second individual intermediate key group which is made up of one of the second system secret keys, and

the second common information generation method includes:

generating encrypted shared keys by encrypting the shared keys based on the second system secret keys which are included in the second system secret key group; and

generating an encrypted shared key group which is made up of encrypted shared keys combined with each other.

6. The key distribution system according to Claim 1, said system further comprising a key distribution center which is connected with

said respective receiving devices via the communication channel and distributes an individual information group,

wherein said key distribution center includes:

an output device information storage unit operable to store one or more individual keys which have been previously provided to said receiving devices;

individual information generation units operable to generate the individual information; and

an individual information group distribution unit operable to distribute the individual information group including at least two types of sets of the individual information and an individual information identifier which corresponds to said individual information generation unit, to said receiving devices simultaneously or at different times,

each of said individual information generation units is operable to output the individual information identifier, the system secret variable group and the individual information based on the individual information generation method which is uniquely used by each of said individual information generation units,

each of said receiving devices includes:

an individual key storage unit operable to store the previously provided individual key;

an individual information group receiving unit operable to receive the individual information group; and

individual intermediate key group obtainment units which correspond to said individual information generation units,

said individual information group receiving units output the individual information corresponding to the individual information identifiers to said respective individual intermediate key obtainment units based on the individual information identifiers included in the received individual information group, and

each of said individual intermediate key obtainment units is operable to obtain the individual intermediate key group based on the individual information and the individual key using an individual intermediate key obtainment method corresponding to the individual information identifier.

7. The key distribution system according to Claim 6,

wherein each of said individual information generation units further generates the system secret variable group,

said key distribution center includes a system secret variable group set sending unit operable to distribute, to said server, the system secret variable group set including two types of sets of the system secret variable group and the individual information identifier which corresponds to said individual information generation unit, and

said server includes a system secret variable group set receiving unit operable to store the distributed system secret variable group sets into said system secret variable group storage unit.

8. The key distribution system according to Claim 6,

wherein said key distribution center is connected to said server via the communication channel,

said system secret variable group set sending unit is operable to distribute the system secret variable group set to said server via the communication channel, and

said system secret variable group set receiving unit is operable to receive the system secret variable group set from said key distribution center via the communication channel.

9. The key distribution system according to Claim 6,

wherein said system secret variable group set sending unit is operable to record the system secret variable group set on a portable medium, and

said system secret variable group set receiving unit is operable to read out the system secret variable group set recorded on the portable medium.

10. The key distribution system according to Claim 7,

wherein said key distribution center and said server are assumed to share a server key in advance,

said system secret variable group set sending unit is operable to generate encrypted data by encrypting the system secret variable group set based on the server key and distribute the server key to said server, and

said system secret variable group set receiving unit is operable to obtain the system secret variable group set by decrypting the distributed encrypted data based on the server key.

11. The key distribution system according to Claim 6,

wherein each individual information generation method includes a first individual information generation method,

each individual intermediate key obtainment method includes a first individual intermediate key obtainment method which is paired with the first individual information generation method,

said key distribution center includes a term information storage unit operable to store one or more types of sets of a previously provided term key, a first system secret variable group, and a term identifier, the first system secret variable group and the term identifier corresponding to the term key,

said individual key storage units of said receiving devices each is operable to store one or more types of sets of a first encrypted individual intermediate key group and a term identifier, the encrypted first individual intermediate key group being generated by encrypting the first individual intermediate key group based on the term key, and the term identifier corresponding to the term key,

the first individual information generation method includes:

selecting a set of a term key, a first system secret variable group and a term identifier which are included in said term information storage unit; and

generating encrypted term keys by encrypting the term keys based on each of the individual keys,

the individual information group includes first individual information which is composed of an encrypted term key group and the term identifier, the encrypted term key group being made up of the encrypted term keys combined with each other, and

the fist individual intermediate key group obtainment method includes:

obtaining the term key by decrypting one of the encrypted term keys which are included in the first individual information; and

selecting the first encrypted individual intermediate key group corresponding to the term identifier from among one or more of the first encrypted individual intermediate key groups included in said individual key storage unit; and obtaining the first individual intermediate key group by decrypting the encrypted first individual intermediate key group based on the term key.

12. The key distribution system according to Claim 6,

wherein each individual information generation method includes a second individual information generation method,

each individual intermediate key obtainment method includes a second individual intermediate key group obtainment method which is paired with the second individual information generation method,

the second individual information generation method includes:

selecting one of the second system secret keys for each of the individual keys; and

generating second encrypted system secret keys by encrypting the selected second system secret key based on each of the individual keys,

wherein, in the second individual information generation method, the individual information group includes second individual information including a second encrypted system secret key group which is made up of the second encrypted system secret keys combined with each other, and

the second individual intermediate key group obtainment method includes:

selecting one second encrypted system secret key corresponding to the individual key from among the second encrypted system secret keys included in the second individual information; and

obtaining the second system secret key by decrypting the selected second encrypted system secret key based on the individual key, the second system secret key being considered as the second individual intermediate key group.

13. The key distribution system according to Claim 2,

wherein the individual intermediate key generation equation includes at least addition operation and multiplication operation.

14. The key distribution system according to Claim 2,

wherein the time variable generation equation includes at least addition operation and multiplication operation.

15. The key distribution system according to Claim 2,

wherein the server shared intermediate key generation equation includes at least addition operation and multiplication operation.

16. The key distribution system according to Claim 2,

wherein said receiving device shared intermediate key generation equation includes at least addition operation and multiplication operation.

17. The key distribution system according to Claim 4,

wherein the second system secret key group is made up of ten second system secret keys.

18. A receiving device in a key distribution system comprising a server which distributes shared keys and receiving devices which receive the shared keys, said receiving device comprising:

a common information receiving unit operable to receive the common information from outside;

an individual intermediate key group storage unit operable to store individual intermediate key group sets each of which is made up of individual intermediate key groups corresponding to each of the common information generation methods;

shared key obtainment units which correspond to said common information generation methods; and

a shared key obtainment unit selection unit operable to select one of the shared key obtainment units,

wherein said shared key obtainment unit selection unit is operable to select the shared key obtainment unit based on the common information identifier included in the common information which has been received by said common information receiving unit, and

said shared key obtainment unit is operable to obtain the shared key, using the common information, based on the shared key obtainment method corresponding to the common information identifier and the individual intermediate key group.

19. The receiving device according to Claim 18,

wherein each shared key obtainment method includes a first shared key obtainment method,

the individual intermediate key group set includes an individual intermediate key group which is made up of one or more first individual intermediate keys,

each of the receiving devices has been provided with one or more receiving device shared intermediate key generation equations,

the common information includes first common information which is made up of a time variable group and an encrypted shared key, and

the first shared key obtainment method includes:

generating the shared intermediate keys based on the time variable group, the first individual intermediate key group and the receiving device shared intermediate key generation equations which are included in the first common information; and

obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

20. The receiving device according to Claim 18,

wherein each shared key obtainment method includes a second shared key obtainment method,

the individual intermediate key group set includes a second individual intermediate key group which is made up of one or more of the second system secret keys,

the common information includes second common information which is made up of an encrypted shared key group including one or more encrypted shared keys, the encrypted shared keys being generated by encrypting the shared keys based on the one or more of the second system secret keys, and

the second shared key obtainment method includes:

selecting one of the encrypted shared keys which corresponds to any of the second system secret keys included in the second individual intermediate key group from among the encrypted shared key group included in the second common information; and

obtaining the shared key by decrypting the selected encrypted shared key based on the second system secret key.

21. The receiving device according to Claim 20,

wherein the individual intermediate key group set includes a second individual intermediate key group which is made up of one of the second system secret keys.

22. The receiving device according to Claim 18,

wherein the key distribution system further comprising a key distribution center which is connected with the receiving devices via the communication channel and distributes an individual information group,

each of said receiving devices includes:

an individual key storage unit operable to store the previously provided individual key;

an individual information group receiving unit operable to receive the individual information group from outside; and

individual intermediate key group obtainment units which correspond to the individual intermediate key obtainment methods,

said individual information group receiving units output the individual information corresponding to the individual information identifiers included in the individual information group to said respective individual intermediate key obtainment units based on the individual information identifiers included in the received individual information group, and each of said individual intermediate key obtainment units is operable to obtain the individual intermediate key group based on the individual information and the individual key using an individual intermediate key obtainment method corresponding to the individual information identifier.

23. The receiving device according to Claim 19,

wherein each individual intermediate key obtainment method includes a first individual intermediate key group obtainment method,

each of said individual key storage units of the receiving devices is operable to store one or more types of sets of a first encrypted individual intermediate key group and a term identifier, the first encrypted individual intermediate key group being generated by encrypting the first individual intermediate key group based on a term key, and the term identifier corresponding to the term key,

the individual information group includes first individual information which is made up of an encrypted term key group and the term identifier, the encrypted term key group including encrypted term keys generated by encrypting the term keys based on the respective individual keys, and

the first individual intermediate key group obtainment method includes:

obtaining the term key by decrypting one of the encrypted term keys included in the first individual information;

selecting one of the first encrypted individual intermediate key groups which corresponds to the term identifier from among one or more of the first encrypted individual intermediate key groups included in said individual key storage unit; and

obtaining the first individual intermediate key group by decrypting the first encrypted individual intermediate key group based on the term key.

24. The receiving device according to Claim 20,

wherein each individual intermediate key obtainment method includes a second individual intermediate key group obtainment method,

the individual information group includes second individual information including a second encrypted system secret key group which is made up of second encrypted system secret keys generated by encrypting one of the second system secret keys based on the respective individual keys, and

the second individual intermediate key group obtainment method includes:

selecting one second encrypted system secret key corresponding to the individual key from among the second encrypted system secret keys included in the second individual information; and

obtaining the second system secret key by decrypting the selected second encrypted system secret key based on the individual key, the second system secret key being considered as the second individual intermediate key group.

25. The receiving device according to Claim 19,

wherein each of the receiving device shared intermediate key generation equations includes at least addition operation and multiplication operation.

26. A program which causes a computer to execute processing of receiving shared keys, the computer being connected with a server which distributes the shared keys via a communication channel, and the processing including:

a reception step of receiving the common information from outside;

a storage step of storing an individual intermediate key group set which is made up of individual intermediate key groups corresponding to the respective shared key obtainment methods;

an obtainment step of obtaining the shared keys corresponding to the shared key obtainment methods; and

a selection step of selecting one of the shared key obtainment units based on the common information identifiers included in the common information which has been received by the common information receiving unit,

wherein said obtainment step includes obtaining the shared keys, using the common information, based on the shared key obtainment method and the individual intermediate key group, the shared key obtainment method corresponding to the common information identifier.

27. The program according to Claim 26,

wherein each shared key obtainment method includes a first shared key obtainment method,

the individual intermediate key group set includes a first individual intermediate key group which is made up of one or more first individual intermediate keys,

each of the programs has been previously provided with one or more receiving device shared intermediate key generation equations,

the common information includes first common information which is made up of encrypted shared keys generated by encrypting the shared keys based on a time variable group and shared intermediate keys, and

the first shared key obtainment method includes:

generating the shared intermediate keys based on the time variable group, the first individual intermediate key group and the receiving device shared intermediate key generation equations, the time variable group being included in the first common information; and

obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

28. The program according to Claim 26,

wherein each shared key obtainment method includes a second shared key obtainment method,

the individual intermediate key group set includes a second individual intermediate key group which is made up of one or more of the second system secret keys,

the common information includes second common information including an encrypted shared key group which is made up of encrypted shared keys, the encrypted shared keys being generated by encrypting the shared keys based on one or more of the second system secret keys, and

the second shared key obtainment method includes:

selecting one of the encrypted shared keys which corresponds to any of the second system secret keys included in the second individual intermediate key group from among the encrypted shared key group which is included in the second common information; and

obtaining the shared key by decrypting the selected encrypted shared key based on the second system secret key.

29. The program according to Claim 28,

wherein the individual intermediate key group includes one of second individual intermediate key groups each of which is made up of one of the second system secret keys.

30. The program according to Claim 27,

wherein each of the receiving device shared intermediate key generation equations includes at least addition operation and multiplication operation.

31. A medium on which the program according to Claim 26 is recorded.

32. A key distribution method comprising:

a key distribution step of generating common information based on each of the shared keys and distributing the common information; and

key reception steps of obtaining the shared keys based on the common information and an individual intermediate key group set,

wherein, in said key reception steps, at least one individual intermediate key group set has been previously provided, the individual intermediate key group set having been selected from among individual intermediate key group sets including at least two different types of individual intermediate key group sets, each of the individual intermediate key group sets including individual intermediate key groups, and each of the individual intermediate key groups being made up of one or more individual intermediate keys which have been generated based on one or more system secret variable groups,

said key distribution step includes:

a shared key storage step of storing the shared keys;

a storage step of storing the system secret variable group sets which are made up of the previously provided system secret variable groups;

generation steps of generating common information based on each shared key;

a selection step of selecting one of the common information generation steps; and

a distribution step of distributing the common information to the receiving devices simultaneously or at different times,

said common information generation steps include: generating, using different common information generation methods respectively, key update data based on the system secret variable group set and the shared key; and generating common information including (a) common information identifiers and (b) the key update data, the common information identifiers respectively corresponding to the common information generation methods,

said key reception steps include:

a reception step of receiving the common information;

a storage step of storing the individual intermediate key group sets each of which is made up of the individual intermediate key groups respectively corresponding to the common information generation methods;

obtainment steps of obtaining shared keys, the steps respectively corresponding to the generation units which generate common information; and

a selection step of selecting one of the shared key obtainment steps based on the common information identifiers included in the common information which has been received by the common information reception units, and

said obtainment steps include obtaining, the shared keys, using the common information based on (a) the shared key obtainment methods respectively corresponding to the common information identifiers and (b) the individual intermediate key group.

33. The key distribution method according to Claim 32,

wherein each common information generation method includes a first common information generation method,

each shared key obtainment method includes a first shared key obtainment method which is paired with the first common information generation method,

each of the system secret variable group sets includes first system secret variable groups each of which is made up of one or more first system secret variables,

each of the individual intermediate key group sets includes first individual intermediate key groups each of which is made up of one or more first individual intermediate keys, the first individual intermediate keys are respectively generated based on the first system secret variable groups and one or more first individual intermediate key generation equations,

in said key distribution step, one or more time variable generation equations and one or more server shared intermediate key generation equations have been previously provided,

in each of said reception steps, one or more receiving device shared intermediate key generation equations have been previously provided,

the first common information generation method includes:

generating a random number group which is made up of one or more random numbers;

generating a time variable group which is made up of one or more time variables based on the random number group, the first system secret variable groups and the time variable generation equations;

generating shared intermediate keys based on the first system secret variable groups, the random number group and the server shared intermediate key generation equations; and

generating encrypted shared keys by encrypting the shared keys based on the shared intermediate keys,

wherein, in the first common information generation method, the key update data includes the time variable group and the encrypted shared keys, and the first shared key obtainment method includes:

generating the shared intermediate keys based on the time variable group, the first individual intermediate key groups and the receiving device shared intermediate key generation equations; and

obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

34. The key distribution method according to Claim 33,

wherein, in said key distribution step, one of the individual intermediate key group sets has been previously provided,

said key reception step includes storing the previously provided individual intermediate key group set,

each common information generation method includes a first common information generation method,

each shared key obtainment method includes a first shared key obtainment method which is paired with the first common information generation method,

each of the system secret variable group sets includes first system secret variable groups each of which is made up of one or more first system secret variables,

each of the individual intermediate key group sets includes first individual intermediate key groups each of which is made up of one or more first individual intermediate keys, the first individual intermediate keys are respectively generated based on the first system secret variable groups and one or more first individual intermediate key generation equations,

said server has been previously provided with one or more time variable generation equations and one or more shared intermediate key generation equations,

in each of said key reception steps, the one or more of the shared intermediate key generation equations have been previously provided, the first common information generation method includes:

generating a random number group which is made up of one or more random numbers;

generating a time variable group which is made up of one or more time variables based on the random number group, the first system secret variable groups and the time variable generation equations;

generating shared intermediate keys based on the first individual intermediate key groups, the random number group and the server shared intermediate key generation equations; and

generating encrypted shared keys by encrypting the shared keys based on the shared intermediate keys,

wherein, in the first common information generation method, the key update data includes the time variable group and the encrypted shared keys, and

the first shared key obtainment method includes:

generating the shared intermediate keys based on the time variable group, the first individual intermediate key groups and the shared intermediate key generation equations; and

obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

35. The key distribution method according to Claim 32,

wherein each common information generation method includes a second common information generation method,

each shared key obtainment method includes a second shared key obtainment method which is paired with the second common information generation method,

the system secret variable group set includes a second system secret key group which is made up of second system secret keys,

the individual intermediate key group set includes second individual intermediate key groups each of which is made up of one or more of the second system secret keys,

the second common information generation method includes:

generating encrypted shared keys by encrypting the shared keys based on each one or more of the second system secret keys which are included in the second system secret key groups; and

generating an encrypted shared key group which is made up of the encrypted shared keys combined with each other,

wherein, in the second common information generation method, the key update data includes the encrypted shared key group, and

the second shared key obtainment method includes:

selecting one of the encrypted shared keys which corresponds to any of the second system secret keys included in the second individual intermediate key group, from among the encrypted shared key group included in the key update data; and

obtaining the shared key by decrypting the selected encrypted shared key based on the second system secret key.

36. The key distribution method according to Claim 35,

wherein the individual intermediate key group set includes a second individual intermediate key group which is made up of one of the second system secret keys.